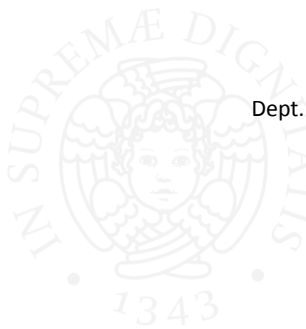
Numerical Attributes and Ciphertext-Policy Attribute-Based Encryption



Marco Rasori
Dept. of Information Engineering
University of Pisa
marco.rasori@ing.unipi.it

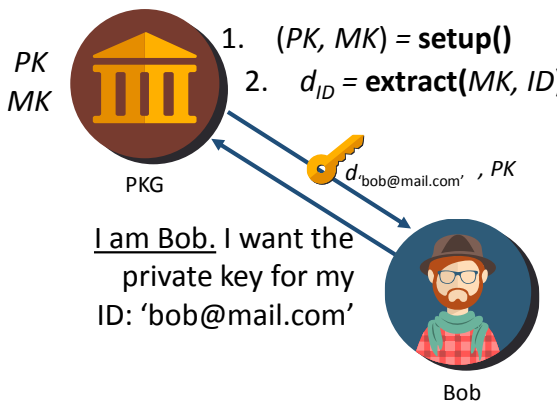
2018-05-04

Recap on IBE and KP-ABE…

Identity-Based Encryption (IBE)

1. (*PK, MK*) = **setup()**

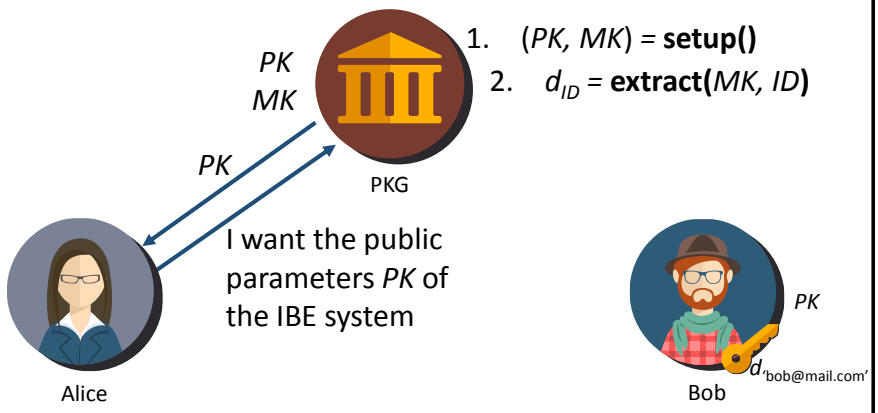
Identity-Based Encryption (IBE)



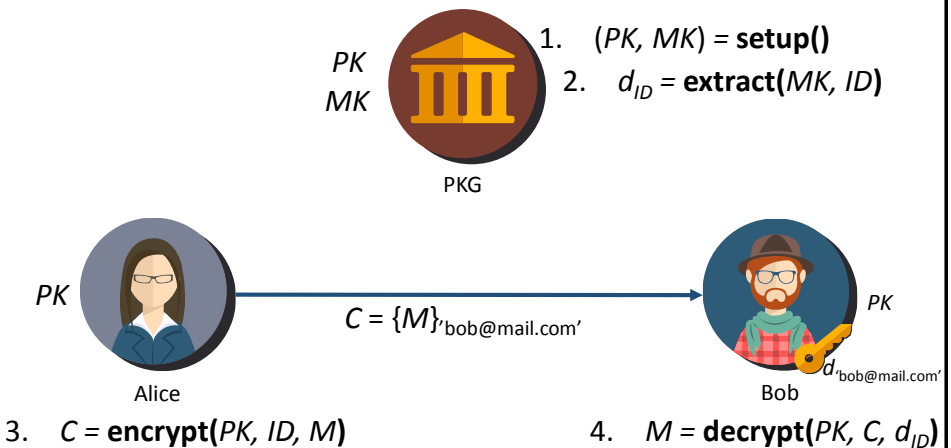
1. (*PK, MK*) = **setup()**
2. d_{ID} = **extract(***MK, ID***)**

$d_{\text{'bob@mail.com'}}$, *PK*

Identity-Based Encryption (IBE)



Identity-Based Encryption (IBE)



KP-ABE

U = *universe of the attributes* e.g., {*A*, *B*, *C*}
γ = *encryption attribute set* e.g., {*A*, *C*}
T = *policy* e.g., *A* OR *B*

PKG

1. (*PK*, *MK*) = **setup(***U***)**
2. *SK* = **keygen(***MK*, *T***)**

Alice

$C = \{M\}_{\gamma}$

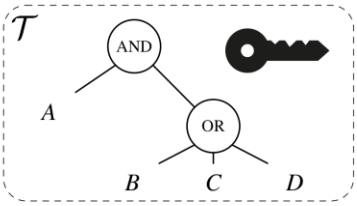
Bob

3. *C* = **encrypt(***PK*, *γ*, *M***)**
4. *M* = **decrypt(***PK*, *C*, *SK***)**

KP-ABE

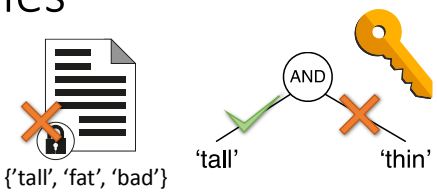
- A **ciphertext** is associated with an attribute set (*encryption attribute set*, *γ*)
- A **private <u>key</u>** is associated with a ***<u>policy</u>*** on the presence of some attributes on the ciphertext (*decryption attribute set*, *λ*)

$\gamma = \{A, C, E\}$

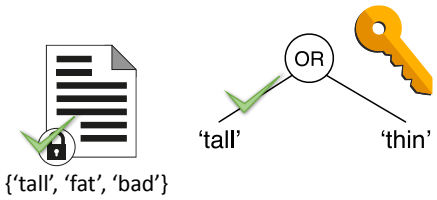


$\lambda = \{A, B, C, D\}$

Examples

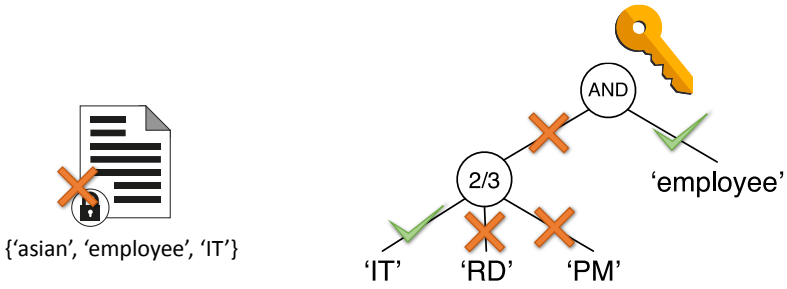


- This key can decrypt a ciphertext if <u>both</u> the attributes 'tall' <u>and</u> 'thin' are associated with the ciphertext.



- This key can decrypt a ciphertext if <u>either</u> the attribute 'tall' <u>or</u> 'thin' is associated with the ciphertext.

Examples



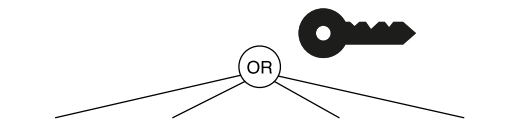
Attributes

Attributes (1/2)

- Each attribute is identified by a string
  - NOT a key-value pair
- For example, if we define ‘profession:student’, “student” is not a value for the key “profession”. Neither “profession” nor “student” are attributes.
- ‘profession:student’ is an attribute.
- ‘italian’ is an attribute.
- ‘year:2018’ is an attribute.

Attributes (2/2)

- Suppose that in a KP-ABE system ciphertexts are associated with the year in which they are produced.
  - e.g., a ciphertext produced in the year 2018 is associated with the attribute ‘year:2018’
- Suppose we want a private key to be valid only for an interval of some years.
  - e.g., the key policy is an OR among the years in which the key is valid



Numerical Attributes (1/4)

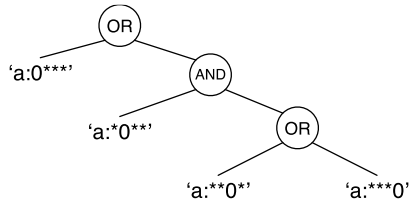
- Integer comparisons
- Binary representation of n-bit integer.
- A *numerical attribute* ‘a’ on 4 bits is implemented by defining 2·n attributes:

‘a:***0’	‘a:***1’
‘a:**0*’	‘a:**1*’
‘a:*0**’	‘a:*1**’
‘a:0***’	‘a:1***’

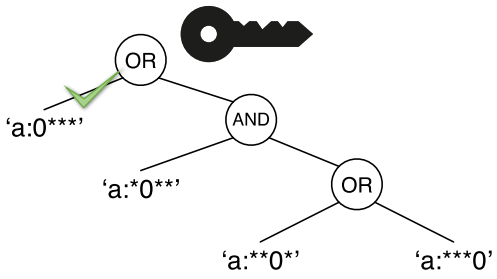
- Two attributes are defined for each bit, one representing the value 0 for that bit, and the other representing the value 1 for that bit

Numerical Attributes (2/4)

- Ciphertext associated with a numerical attribute ‘a’ equal to 5:
  - Binary representation for the integer 5 on 4 bit: 0101
  - The ciphertext is thus associated with the attribute set:
    - {‘a:0***’, ‘a:*1**’, ‘a:**0*’, ‘a:***1’}
- Private key associated with a policy implementing the integer comparison ‘a’ lower than 11:



Numerical Attributes (3/4)

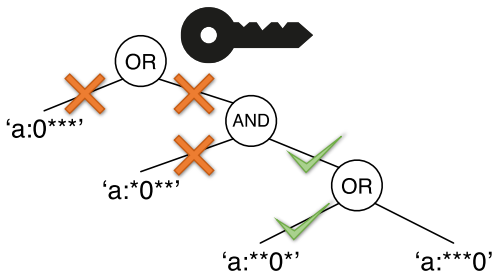


a < 11

{‘a:0***’, ‘a:*1**’, ‘a:**0*’, ‘a:***1’}

a = 5

Numerical Attributes (4/4)



a < 11

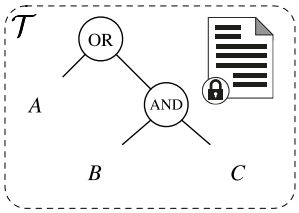
{'a:1***', 'a:*1**', 'a:**0*', 'a:***1'}

a = 13

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

CP-ABE

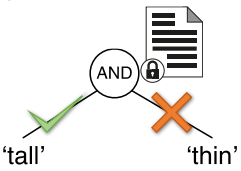
- A **ciphertext** is associated with a *policy* on the presence of some attributes on the private key (*encryption attribute set*, γ)
- A **private key** is associated with an attribute set (*decryption attribute set*, λ)



$\gamma = \{A, B, C\}$

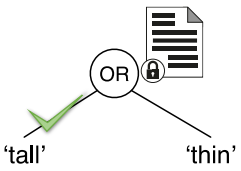
$\lambda = \{B, C, D\}$

Examples



{'tall', 'fat', 'bad'}

- This ciphertext can be decrypted by private keys associated with both the attributes 'tall' and 'thin'.



{'tall', 'fat', 'bad'}

- This ciphertext can be decrypted by private keys associated with either the attribute 'tall' or 'thin'.

CP-ABE Algorithms (1/2)

1. **setup**. This algorithm generates the *public parameters* and a *master key*, which is kept secret.
2. **keygen**. This algorithm uses the master key to generate the *private key* associated to a decryption attribute set λ.

1. (*PK, MK*) = **setup()**
2. *SK* = **keygen(***MK, λ***)**

Notation:

PK	public parameters
MK	master key
SK	private key
λ	decryption attribute set

CP-ABE Algorithms (2/2)

3. **encrypt**. This algorithm takes as input the public parameters, a *message M*, and a policy *T*, which is defined over the encryption attribute set γ. It returns a *ciphertext C*.
4. **decrypt**. It takes as input a ciphertext *C*, and a private key *SK*. It returns the *message M* if the private key is able to decrypt the ciphertext, $\perp$ otherwise.

3. *C* = **encrypt(***PK, M, T***)**
4. *M* = **decrypt(***C, SK***)**

Notation:

PK	public parameters
SK	private key
T	policy
M	message
C	ciphertext

Exercise (1/3)

By using the **kpabe toolkit** installed on VictimOS, implement a KP-ABE system in which students of Computer Engineering evaluate their professors and assistants.

The software asks for the name of the course, the name of the professor/assistant to be evaluated, the evaluation (a grade from 1 to 10), and notes. Then, the software asks if the notes are confidential or non-confidential.

The software creates two ciphertexts; one containing the evaluation, and the other containing the notes. Both the ciphertexts are associated with the attributes representing the course name, the professor/assistant name, and, optionally, the attribute 'Nonconfidential', e.g., {'Cybersecurity', 'GianlucaDini', 'NonConfidential'}. The ciphertext containing the notes lacks of the attribute 'Nonconfidential' if the notes are considered confidential.

Exercise (2/3)

The subjects able to see the evaluations given by the students are the *professors*, the *assistants*, and the *head of master program*.

- The head of master program is provided with a private key which let him/her decrypt all the non-confidential ciphertexts related to all the courses of Computer Engineering.
- A professor is provided with a private key which let him/her decrypt ciphertexts related to the courses he/she teaches. Moreover, he/she can also access the non-confidential ciphertexts related to his/her assistants.
- An assistant is provided with a private key which let him/her decrypt both confidential and non-confidential ciphertexts related to him/her.

Exercise (3/3)

Write the software for the evaluation in C and use the kpabe-enc command within the code.

- Play the role of the TTP: setup the system and generate proper private keys for the parties.
- Play the role of the student: run the evaluation software which generates the ciphertexts.
- Play the role of the different key holders: verify that, according to the policies described above, each subject can decrypt only the portion of data he/she should be authorized to.

Exercise - Extension

- By using numerical attributes, introduce a validity period for the private keys.
  - The head of master program mandate lasts 5 years and started in 2016.
  - Professors and assistants private keys are renewed yearly.
- Ciphertexts include the year in which they have been produced.